Department of Homeland Security Daily Open Source Infrastructure Report for 06 April 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports guards were increasing patrols after a cut was discovered in a security fence at the Paducah Gaseous Diffusion Plant in Paducah, Kentucky. (See item 1)
- The Congress Daily reports Kip Hawley, director of the Transportation Security Administration, said when testifying at a Senate hearing, that additional levels of security must be built into what has become the nation's rigid, static, and predictable airline passenger system. (See item 19)
- The San Francisco Chronicle reports fire hydrants that can be used for emergency drinking water will be marked with a blue water−drop symbol as part of a new program being developed to make sure people can acquire drinking water after an earthquake or other catastrophic disaster. (See item 29)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 05, Associated Press* — **Cut discovered in fence at Kentucky nuke plant.** Guards were increasing patrols after a cut was discovered in a security fence at the Paducah Gaseous Diffusion Plant in Paducah, KY. The three−foot cut was discovered Monday night, April 3,

USEC Inc. spokesperson Elizabeth Stuckle said. USEC leases the plant from the federal government and enriches uranium into nuclear fuel. There was no indication that anyone was trying to take nuclear material, Stuckle said.
Source: http://www.wave3.com/Global/story.asp?S=4730124&nav=0RZF

2. *April 04, Nuclear Regulatory Commission* — **NRC increases the amount of security−related information released as part of its reactor oversight process.** The Nuclear Regulatory Commission (NRC) on Tuesday, April 4, approved a staff recommendation to make more security−related information public as part of the agency's Reactor Oversight Process (ROP). Previously, selected information concerning security reviews of commercial nuclear power plants was considered sensitive information and not released. The ROP monitors performance at nuclear power plants in three areas: reactor safety, radiation safety, and safeguards, which includes security. According to a directive from the Commission, the cover letters for future security inspection reports would be made publicly available. The cover letter would contain a summary statement of the security inspection and indicate whether security findings were identified at the plant. The statement would also indicate that the identified deficiencies had been promptly corrected or actions had been taken to compensate for the problem. The statement would not, however, describe specific security issues that had been identified, as that information may be detrimental to the security of the facility.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 46.html

3. *April 04, Nuclear Regulatory Commission* — **NRC uses risk insights to revise mitigating systems category in reactor oversight process.** The Nuclear Regulatory Commission (NRC) has updated its Reactor Oversight Process (ROP) with the introduction of the Mitigating Systems Performance Index (MSPI), which tracks the availability and reliability of systems used to reduce the severity of incidents at a nuclear power plant. The agency created the ROP six years ago to improve its inspection and enforcement programs for commercial nuclear power plants. At that time, the process included performance indicators for safety system unavailability, but ongoing experience with the ROP revealed the need for further enhancement. The MSPI addresses this need and takes into account plant−specific features. Jim Dyer, Director of the NRC's Office of Nuclear Reactor Regulation, said "This change will improve our ability to track how well utilities are running their plants."
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 45.html

4. *April 04, Associated Press* — **Pacific Energy to build oil pipeline.** Pacific Energy Partners LP on Tuesday, April 4, said it signed a deal with Frontier Oil Corp. to build a new crude oil pipeline system in exchange for petroleum transportation services. Pacific Energy said its Rocky Mountain Pipeline System LLC will construct a pipeline for Frontier spanning from Guernsey, WY, to Laramie and finally to Frontier's refinery in Cheyenne. Frontier agreed to a 10−year commitment to ship 35,000 barrels per day for Pacific Energy. The pipeline will have an initial capacity of 55,000 barrels of heavy crude per day, Frontier said. Capacity can be increased to 90,000 barrels a day.
Source: http://biz.yahoo.com/ap/060404/pacific_energy_frontier.html? .v=1

5. *April 04, Associated Press* — **Feds say Indian Point nuclear complex can brace for air attack.** Federal officials assured Congress on Tuesday, April 4, that Indian Point and other nuclear power plants can quickly change internal operations to protect the public from radiation

exposure if the U.S. military warns a hijacked plane is headed toward a reactor. The assurances came at a House Government Reform subcommittee hearing. Recently, evidence in the death penalty trial of al Qaeda member Zacarias Moussaoui showed the terror group considered attacking a nuclear power plant in Pennsylvania as part of the 2001 wave of airline hijackings, a detail repeatedly mentioned in the hearing. Members of the Nuclear Regulatory Commission said that the agency has several safety measures in place to reduce the impact of such an attack. Commissioner Edward McGaffigan Jr. said the nation's nuclear power system had a contingency plan with U.S. military officials who monitor airspace to get a quick warning if a hijacked airliner is speeding toward a power plant.
Source: http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--indianpoint0404apr04,0,5133932.story?coll=ny-region-apnewyork

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *April 05, Florida Times-Union* — **Ammonia leak snarls traffic, closes access to ferry.** An ammonia tank leak, the result of a puncture caused by demolition work, closed access to the Mayport Ferry and a section of Ocean Avenue in Mayport, FL, for about 90 minutes Wednesday, April 5, to allow cleanup. No evacuations were necessary.
Source: http://www.jacksonville.com/tu-online/stories/040506/met_may port.shtml

[Return to top]

Defense Industrial Base Sector

7. *April 05, Aviation Now* — **Senate appropriators boost funding for C-17, Osprey.** Senate appropriators on Tuesday, April 4, went a step further than their House counterparts to protect the C-17 aircraft, recommending $227.5 million toward advance procurement for more of the heavy lifters in fiscal 2008. The move -- part of the Senate Appropriations Committee's (SAC) version of the latest Bush administration request for supplemental funding for Iraq, Afghanistan and several other efforts such as Gulf Coast hurricane recovery -- follows the full House's move last month to appropriate just $100 million for the C-17. In addition, the SAC included $230 million in unrequested funds to buy three V-22 Osprey tiltrotor aircraft. The House did not do the same. The SAC said procurement of replacement aircraft should be accelerated, especially to support the Marines Corps. Speeding up acquisition of MV-22s will do that, as well as maybe lower costs, the committee said.
Source: http://www.aviationnow.com/avnow/news/channel_defense_story.jsp?id=news/OSP04056.xml

8. *April 05, Defense News* — **Pentagon adopts tougher policy on contractor bonuses.** The Pentagon’s No. 2 procurement official, James Finley, told the Department of Defense's acquisition work force in a new policy memo there will be no more awards for contractors who do a less-than-satisfactory job. Procurement officials must set better milestones to measure contractor performance and clarify how they’ll evaluate it, the Wednesday, March 29, memo said.

Source: http://www.defensenews.com/story.php?F=1665548&C=america

9. *April 05, Congress Daily* — **Navy secretary says shipbuilders need long−term focus.** Navy Secretary Donald Winter told the shipbuilding industry Tuesday, April 4, to get beyond its short−term focus on its earnings and think more of the long term and national interests. Addressing an audience heavy with defense industry representatives at the Wardman Park Marriott, Winter noted the Navy's recently released "ambitious, comprehensive" 30−year shipbuilding plan that promises to build the fleet up to 313 ships from the current 281. But to make that plan work, he said, "we need a better alignment between the industry and the Navy. From where I sit today, I see diverging interests."
Source: http://www.govexec.com/story_page.cfm?articleid=33760&dcn=to daysnews

10. *April 05, Government Accountability Office* — **GAO−06−585T: Defense Acquisitions: Actions Needed to Get Better Results on Weapon Systems Investments (Testimony).** In the past five years, the Department of Defense (DoD) has doubled its planned investments in weapons systems, but this huge increase has not been accompanied by more stability, better outcomes, or more buying power for the acquisition dollar. Rather than showing appreciable improvement, programs are experiencing recurring problems with cost overruns, missed deadlines, and performance shortfalls. The Government Accountability Office (GAO) was asked to testify on ways to obtain a better return on DoD's weapons systems investments. This testimony identifies the following steps as needed to provide a better foundation for executing weapon programs: (1) developing a DoD−wide investment strategy that prioritizes programs based on realistic and credible threat−based customer needs for today and tomorrow, (2) enforcing existing policies on individual acquisitions and adhering to practices that assure new programs are executable, and (3) making it clear who is responsible for what and holding people accountable when these responsibilities are not fulfilled. Past GAO reports have made similar recommendations.
Highlights: http://www.gao.gov/highlights/d06585thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−585T

11. *April 04, U.S. Department of State* — **Missile Defense Agency requests $9.3 billion for 2007.** The U.S. Missile Defense Agency's continuing effort to develop, test and deploy a joint, integrated, and multi−layered ballistic missile defense system will cost $9.3 billion in fiscal year 2007, the director of the program says. In prepared testimony for a Senate Armed Services subcommittee Tuesday, April 4, Air Force Lieutenant General Henry Obering III said that figure represents a requested increase of $1.6 billion over the fiscal year 2006 funding level.
Obering's testimony: http://armed−services.senate.gov/statemnt/2006/April/Obering%2004−04−06.pdf
Source: http://usinfo.state.gov/xarchives/display.html?p=washfile−english&y=2006&m=April&x=20060404165451adynned0.8707697&t=live feeds/wf−latest.html

[Return to top]

Banking and Finance Sector

12. *April 05, The Register (UK)* — **Trojan−powered scam network dismantled.** Banks,

telecommunication companies, hotels, airlines, and international betting services were among those affected by the creation and sale of Briz Trojans, a malware−creation−for−hire scam recently uncovered by security researchers. The racket was exposed following analysis of a recently discovered Trojan, Briz−A, which revealed the existence of a complex system dedicated to creating and selling of à la carte malware designed for stealing personal and confidential data. The information stolen by the Trojan was stored in 2,033 files occupying 70.6MB. The files were organized into folders corresponding to the nationality of each victim. “We were surprised by the quantity of data that a single one of these Trojans was able to steal... We don't know how many were generated or sold before the system was dismantled, and so the number of companies whose data is now in jeopardy could be very high,” said Luis Corrons of PandaLabs. He added: "The sale of customized malware to cyber−crooks has now become a lucrative business model. This is not an isolated case and given the lure of financial gain motivating cyber−criminals, this type of scam is likely to proliferate in the short−term."
Source: http://www.theregister.co.uk/2006/04/05/trojan_scam_network_dismantled/

13. *April 05, Associated Press* — **China fines 600 financial institutions.** China fined 600 financial institutions a total of $7 million for money−laundering violations in 2005. The Chinese central bank's center for monitoring and analyzing suspected money laundering said it reviewed suspect transactions worth about $10.8 billion in 2005, China Business News reported, citing People's Bank of China statistics. China has been gradually tightening controls and raising disclosure requirements for banks and other financial institutions, amid estimates that the scope of money laundering has grown to as much as $50 billion a year. The number of institutions suspected of violations rose sharply last year from 2004, when 66 financial institutions paid fines totaling more than $212,000, the report said.
Source: http://www.nytimes.com/aponline/business/AP−China−Money−Laundering.html?_r=1&oref=slogin

14. *April 05, Websense Security Labs* — **Phishing alert: AA Savings.** Websense Security Labs has received reports of a new phishing attack that targets customers of AA Savings. Users receive a spoofed e−mail that asks them to review and update their account details. The message provides a link to a phishing Website. Users who visit this Website are prompted to enter their account number, password and Memorable word.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =457

15. *April 05, Websense Security Labs* — **Malicious Website / Malicious Code: New Trojan banker technique.** Websense Security Labs has received reports of a Trojan Horse that uses a new technique to steal financial account information. The Trojan monitors Microsoft Internet Explorer and waits for the user to visit one of a dozen financial Websites. Once the user begins the logon process, the Trojan creates a pop−up window to replace the actual logon page. These pop−up windows are customized for each Website and designed to spoof the appearance of the legitimate logon page. Account information entered into these pop−up windows is captured and e−mailed to the attacker.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =458

16. *April 04, KGO TV 7 (CA)* — **Man suspected of using iPod to store stolen IDs.** Instead of storing songs on his iPod, the San Francisco Police Department says a man was storing credit cards, social security numbers, and other stolen information on his music player. The number of

victims may reach a thousand. The man has been charged with 54 criminal counts including identity thefts, credit card fraud, and forgery. The suspect had a list of more than 500 credit card numbers, including one stolen from a congressperson, another from a federal law enforcement agent, social security cards, and 60 to 70 credit reports filled with people's financial data. Lt. Kenwade Lee of the San Francisco Police Department said 35−year−old Wilson Lee was arrested after a six−month investigation into a series of identity thefts. Lt. Lee says the suspect also had reams of unsigned student loan applications submitted online as well as financial letters of authorization. He also had obtained credit reports from finance companies from people that were either refinancing homes or purchasing homes.
Source: http://abclocal.go.com/kgo/story?section=local&id=4055150

17. *April 04, TechWeb News* — **Germany arrests phishing gang.** German federal police on Tuesday, April 4 arrested seven members of a suspected phishing gang on fraud charges after a three−month investigation. According to the Website of Germany's Federal Crime Office, known as the Bundeskriminalamt, or BKA, police nabbed seven men, ages 21 through 47, who were allegedly plotting to spamming password−stealing Trojans to online bank customers. The gang, which included both Germans and Lithuanians, had already opened numerous accounts using bogus names and addresses, and planned to transfer the proceeds of their phishing to Eastern European accounts.
Source: http://www.techweb.com/wire/security/184428438;jsessionid=T5R3ZFT1H0TSIQSNDBOCKICCJUMEKJVN

18. *April 04, Websense Security Labs* — **Phishing Alert: Multiple Italian banks.** Websense Security Labs has received reports of a new phishing attack that targets customers of four Italian banks. The banks targeted are: Credem, Banca Carige, Credito Valtellinese, and RAS Bank. Users are lured into a fake login page and are asked to provide login details. All four URLs redirect to the same Web server, which redirects the main window of the legitimate bank sites after user details have been provided.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =456

[Return to top]

Transportation and Border Security Sector

19. *April 05, Congress Daily* — **TSA official says airport security is too predictable.** Additional levels of security must be built into what has become the nation's "overly rigid, static and predictable airline passenger system," a top federal official testified Tuesday, April 4, at a Senate hearing. "Terrorists can more easily 'engineer around' these highly structured defenses," Kip Hawley, director of the Transportation Security Administration (TSA), told the Senate Commerce Committee. Hawley said his agency now focuses more on finding improvised explosive devices and continues to install bomb−testing devices at airports. TSA also has begun developing a plan to train screeners to use behavior recognition techniques and have assigned employees trained in those techniques at 10 high−risk airports, Hawley said. In a recent pilot program, if a passenger was identified as exhibiting behaviors indicative of fear, stress, or deception, they were either referred to additional screening, or referred for selective screening or an evaluation interview. Cathleen Berrick, director for homeland security and justice for the Government Accountability Office, also cited other issues with baggage screeners including

training problems and a high turnover rate, reaching 50 percent for the system's part−time workers, likely a result of low pay and work−related injuries.
Source: http://www.govexec.com/story_page.cfm?articleid=33756&dcn=to daysnews

20. *April 05, Associated Press* — **Chicago officials propose plan to stop runway overruns at Midway.** The city of Chicago has submitted a $40 million proposal to the Federal Aviation Administration (FAA) to build lightweight concrete beds at Midway Airport to help prevent planes from overshooting their landings, officials said. The plan comes four months after a Southwest Airlines flight skidded off a runway at Midway and into traffic, killing six−year−old Joshua Woods of Leroy, IN, who was riding in a nearby car. The concrete beds are made of lightweight bricks designed to collapse under the weight of an aircraft, safely slow planes' acceleration, and are heavy enough for people to walk on, according to the manufacturer. Under the plan, which was submitted Tuesday, April 4, each bed would be between 200 and 300 feet. The FAA has approved similar systems at 14 airports, officials said, and seven more are being designed or planned. If the FAA approves Chicago's proposal, construction could begin as early as this year, said Erin O'Donnell, managing deputy aviation commissioner at Midway.
Source: http://www.usatoday.com/travel/flights/2006−04−05−midway−run way_x.htm

21. *April 05, Associated Press* — **US Airways plane apparently hits bird in flight, lands safely.** A US Airways flight apparently hit a bird Tuesday night, April 4, as it approached Seattle−Tacoma International Airport, causing flashes in an engine that alarmed some people both on board the plane and on the ground. The plane carrying 114 people landed safely and no injuries were reported, airline spokesperson Valerie Wunder confirmed in a telephone interview from Tempe, AZ. Wunder said a bird apparently hit the engine, which can cause a sort of backfire effect.
Source: http://www.usatoday.com/travel/flights/2006−04−05−plane−bird_x.htm

22. *April 05, Associated Press* — **Venezuela: Airline halts planned flight.** Venezuela, which is seeking to regain its own airlines' access to the United States, said on Tuesday, April 4, that American Airlines could not add a planned fourth daily flight to Miami from Caracas. The country's aviation authority said it notified the carrier last week that it needed government authorization to restore a fourth flight that was eliminated in January after a highway between Caracas and Venezuela's main airport was temporarily closed. American's parent, AMR Corp., said Monday, April 3, that it would not restore the fourth flight to Miami as planned and refunded tickets. In 1995, the United States imposed safety restrictions prohibiting Venezuelan airlines from flying their own planes to the U.S. or from launching new services such as expansions or changes in routes. Last week Venezuela's Infrastructure Ministry set an April 25 deadline by which the U.S. Federal Aviation Administration must drop restrictions against Venezuelan carriers or face retaliatory measures.
Source: http://biz.yahoo.com/ap/060404/venezuela_us_airlines.html?.v =2

23. *April 05, Canadian Press* — **Canada, U.S. may share databases to guard borders.** Canada and the United States are talking about sharing databases of information to check the identity of each other's residents as they cross the border. Jim Williams, director of the U.S.−VISIT program in the Department of Homeland Security, says both countries are concerned about providing each other with the data, but that so far discussions are in the early stages. Williams says the U.S. is hoping Canada agrees to devise a new card with proof of citizenship like the

one being developed south of the border, adding that it may be a quicker way to clear border checks than even a passport.
Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060405/broder_databases_cp_060405/20060405?hub=Canada

24. *April 04, Cox News Service* — **Electrical outage disrupts Atlanta airport.** A power outage hit one of Hartsfield−Jackson International Airport's gate concourses Monday afternoon, April 3, forcing airlines to shift planes to other concourses, delay flights, or resort to manual processing of passengers. The outage hit Concourse D when a construction worker inadvertently cut an electrical line, spokesperson Felicia Browder said. Five other concourses at the world's busiest airport were not affected. AirTran Airways, which has nine gates on Concourse D, had the most flights affected, Browder said. Several other airlines also operate from D, including Delta Connection carriers Atlantic Southeast Airlines and Comair, along with Continental, Midwest, Northwest, and US Airways. Hundreds of passengers milled about or waited in chairs on the concourse Monday afternoon. Extra security personnel were stationed in the concourse.
Source: http://www.pulsejournal.com/sports/content/shared/news/stories/ATL_AIRPORT_OUTAGE_0404_COX.html

25. *April 04, Department of Justice* — **The Federal Bureau of Investigation's efforts to protect the nation's seaports.** The Department of Justice Office of the Inspector General (OIG) initiated this audit to examine the Federal Bureau of Investigation's (FBI) seaport security efforts. OIG reviewed the FBI's roles and responsibilities for preventing and responding to terrorist attacks in the maritime domain, and the extent and effectiveness of the FBI's interagency coordination and cooperation. To accomplish these overall objectives, OIG examined the FBI's: (1) initiatives to prevent maritime terrorism, including coordination with the Coast Guard and other agencies; (2) capability to respond to maritime incidents; and (3) efforts to assess the maritime terrorism threat. The OIG has concluded that unless incident command and other coordination issues are resolved in advance and response scenarios are exercised, the overlapping nature of the FBI's and the Coast Guard's responsibilities in the maritime domain may result in confusion and interagency conflict with the FBI in the event of a maritime incident.
Source: http://www.usdoj.gov/oig/reports/FBI/a0626/final.pdf

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

26. *April 05, Information Society Technologies* — **New crop of technology reveals plant health.** Scientists have developed a system that picks up the subtle cues of plant communication helping plant growers to monitor the crop’s state of health. Funded under the European Commission’s FET (Future and Emerging Technologies) initiative, the PLANTS project sought

to develop a unique system that linked plants, technology and people to continuously assess the state of crop health. Using sensors, transmitters and specialist software, the system monitors the state of the crop on a plant−by−plant basis, in near real−time. The system uses an infrared camera to scan the entire crop canopy. It can automatically detect when individual or groups of plants are getting too hot. Another sensor detects chlorophyll fluorescence, which tells the system the rate at which the plant is absorbing energy. That reflects the current state of photosynthesis, itself a reflection of the plant's health. These sensors communicate their data through specially developed wireless transmitters.
Source: http://istresults.cordis.lu/index.cfm/section/news/tpl/article/ID/81342/BrowsingType/Features

27. *April 04, Associated Press* — **Senate committee approves agriculture disaster aid.** Farm−state members successfully attached an estimated four billion dollars in agricultural disaster money Tuesday, April 4, to a massive spending bill designed to pay for the Iraq war and Hurricane Katrina. The bill would pay farmers and ranchers around the country for recent losses due to drought, flooding, disease and other disasters. It would also give many farmers an increase on their current federal subsidy check because of higher energy expenses. Missouri and Kansas lawmakers called the money critical for states where several years of drought have decimated row crops and reduced water supplies for livestock. The bill would provide assistance to farmers around the country, including those who have suffered losses due to Hurricane Katrina, wildfires in Texas and flooding in Hawaii, North Dakota and California.
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/politics/14263224.htm

[Return to top]

Food Sector

28. *April 05, Chosun Ilbo (South Korea)* — **U.S. failure to prove infected cow's age could halt imports.** South Korea says the U.S. has failed to prove its claim that a cow found infected with mad cow disease last month is 10 years old. That would jeopardize South Korea's resumption of beef imports from the U.S. since the two sides agreed in negotiations in January that Korea can suspend imports again if U.S. cattle born after April 1998 come down with mad cow disease.
Source: http://english.chosun.com/w21data/html/news/200604/200604050029.html

[Return to top]

Water Sector

29. *April 04, San Francisco Chronicle* — **Hydrants marked for drinking water.** Fire hydrants that can be used for emergency drinking water will be marked with a blue water−drop symbol as part of a new program being developed by San Francisco, CA, officials as part of a one million dollar program to make sure people can acquire drinking water after an earthquake or other catastrophic disaster. Hydrants that dispense potable water are at 67 locations throughout the city. Officials hope to have them all marked by April 18.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/04/04/BAG22I1R2L1.DTL

[Return to top]

Public Health Sector

30. *April 05, Southern (IL)* — **Area health officials worried about possible mumps outbreak.** A confirmed case of mumps in Franklin, IL, has area health officials concerned about the possibility of the recent Midwest epidemic hitting Southern Illinois. An infection long considered dormant, mumps cases have been cropping up throughout Iowa, which has seen as many as 300 confirmed cases within recent days. Mumps has steadily moved across Missouri, Wisconsin, and Kansas, which reported nine confirmed cases within Douglas County on Tuesday, April 4. Only one case of mumps has been confirmed within the area, but health departments say they are dealing with some suspected mumps cases as well.
Mumps information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mumps.htm
Source: http://www.southernillinoisan.com/articles/2006/04/05/top/doc4433ac350ab67200655224.txt

31. *April 05, Washington Post* — **Food and Drug Administration warns maker of anthrax vaccine.** Federal drug regulators have accused a California company of breaking the law by making exaggerated claims about the purity and effectiveness of a new vaccine for anthrax. The U.S. Food and Drug Administration (FDA) accused VaxGen Inc. of making "false or misleading statements" about the vaccine, essentially by offering rosy interpretations of the handful of scientific studies that have been completed on the product. The FDA specifically cited a promotional document the company handed out in October that claimed the company's techniques allowed it to produce a vaccine "at nearly 100 percent purity" and asserting that the product generates immunity comparable to that induced by an older vaccine. Neither claim is warranted on the basis of early research, the FDA declared.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/04/AR2006040401725.html

32. *April 05, Reuters* — **Bird flu kills child in Cambodia.** The death of a boy of 12 in Cambodia and the case of a sick baby girl in Egypt underlined on Wednesday, April 5, the threat posed to children by the H5N1 bird flu virus. In Europe, experts called for new precautions because cats, and possibly other mammals, can be infected and could spread the virus. Germany said that tests had shown a form of H5N1 had spread to domestic fowl on a large farm in the eastern state of Saxony. In the latest case in Cambodia, a boy from the southeastern province of Prey Veng, abutting Vietnam, died on Tuesday, April 4, said Michael O'Leary, the World Health Organization representative. Egypt said its latest human case was a baby girl from the south of the country whose father raised birds in his home. Germany said it would start culling to prevent the spread of bird flu after finding it on a farm which houses more than 16,000 turkey, geese and chickens.
Source: http://msnbc.msn.com/id/12166286/

33. *April 05, Agence France−Presse* — **Singapore plans two−day drill, guidebooks to prepare for bird flu pandemic.** Singapore will hold a two−day drill in July to test the city−state's readiness to cope with a bird flu pandemic, officials have said. The drill will involve a hospital, clinics and doctors where the aim is to test out infection control measures, temperature

screening procedures and simulated treatment of probable cases of bird flu. Plans are also under way to mail more than one million copies of a handbook guide on bird flu to households by the end of the month. The handbook details the symptoms of the disease and precautionary measures to take, among other things. Singapore has so far been spared from the bird flu outbreak that has hit other Southeast Asian.
Source: http://news.yahoo.com/s/afp/20060405/hl_afp/healthflusingapore_060405062752;_ylt=AileqvScpgQCfDHD8kb6JQSJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

34. *April 04, Reuters* — **Canadian police probe theft of HIV−tainted blood.** Canadian police and health officials searched on Tuesday, April 4, for a thief who made off with vials of HIV−contaminated blood plasma from a Vancouver hospital. The thief pried open a locked freezer at a laboratory at St. Paul's Hospital during the weekend and removed the 19 vials that were marked with the lettering "HIV VL" and labeled with the patients' names, police said.
Source: http://www.alertnet.org/thenews/newsdesk/N04206537.htm

35. *April 03, Government Computer News* — **North Carolina puts out a net for tracking diseases.** When Hurricane Katrina evacuees reached North Carolina last year, public health officials tracked the resulting surge in emergency room visits via a standards−driven statewide biosurveillance network. The project, known as the North Carolina Disease Event Tracking and Epidemiological Collection Tool (NC−DETECT), is an example of the kind of biosurveillance system that the U.S. Health and Human Services Department is looking for as part of its early use of health IT. NC−DETECT is the syndromic surveillance arm of the state's Public Health Information Network. It's designed to be the canary in the coal mine, providing early alerts of public health problems to providers and health care planners. North Carolina public health professionals have used NC−DETECT to track the state's flu season. It can provide information on occupational health risks. And it is designed to detect bioterrorism and events such as a potential avian flu outbreak. NC−DETECT includes data collected by the North Carolina Hospital Association in accord with a state mandate requiring hospitals to transmit selected emergency department data elements to the state at least daily.
Source: http://www.gcn.com/print/25_7/40291−1.html

[Return to top]

Government Sector

36. *April 05, Associated Press* — **Teenage girl arrested with drugs in courthouse.** A 16−year−old girl arrested for carrying marijuana and cocaine into a northwestern Indiana courthouse said she was holding the drugs for her boyfriend. Security guards stopped the girl Monday, April 3, when a metal detector went off as she walked through it at the Porter County Courthouse. When a guard checked the girl's coat, she found a plastic bag filled with what appeared to be marijuana and cocaine, police said. The girl told police she was holding the drugs for her 22−year−old boyfriend who was meeting with his probation officer, police said.
Source: http://www.fortwayne.com/mld/newssentinel/news/local/14269637.htm

[Return to top]

Emergency Services Sector

37. *April 05, West Virginia Gazette* — **West Virginia National Guard participates in dirty bomb drill.** If a terrorist organization set off a nuclear device in the nation's capital, specially trained units from the West Virginia National Guard would probably be called in to rescue, decontaminate and give medical aid to victims. To prepare for such an event, 107 members of the West Virginia National Guard took park in a drill, called "Operation Vital Guardian," held in Washington, DC, Tuesday, April 4. The drill simulated a dirty bomb detonation at an outdoor sports arena by a mock terrorist group, the United Adversary. The simulation was held across the street from RFK Stadium, on the grounds of the National Guard Armory. National Guard members from nine states and the District of Columbia took part. "It's a great opportunity for us to work with all these other people from other states, and find out what our strengths and weaknesses are," said Maj. Kim Sencindiver, medical operations officer for the Chemical, Biological, Radiological, Nuclear and High Yield Explosive Emergency Response Force team.
Source: http://wvgazette.com/section/News/2006040425

38. *April 05, Pueblo Chieftain (CO)* — **Digital radios tested in security run.** A small−scale test was held Saturday, April 1, for a new network of 900 digital radios provided to law enforcement, fire and emergency medical departments in the San Luis Valley, CO. Jeff Babcock, San Luis Valley Regional Homeland Security coordinator, called the exercise, which involved emergency workers in Alamosa and Conejos counties, a success. In the past three years, between $4.5 million and $5 million has been spent on the 900 mobile, portable and base station radios and infrastructure. Two towers, at Monte Vista and San Luis, are expected to be up and running in about a month and two additional towers, at Creede and at Wolf Creek, are expected to be functional by late fall, Babcock said. "The radios function real well. There are some programming issues but these can be worked out," Babcock said.
Source: http://www.chieftain.com/metro/1144245619/12

39. *April 04, Herald−Dispatch (WV)* — **Fifth annual Multiple Death Disaster Management Symposium underway.** The Tri−State Fire Academy, the West Virginia Funeral Directors Association and several other emergency response agencies began their fifth annual three−day Multiple Death Disaster Management Symposium Tuesday, April 4, in Huntington, WV. The program reflects the interdisciplinary nature of disaster management and will feature discussions between all groups involved −− including coroners and medical examiners, funeral directors, firefighters, emergency medical responders, law enforcement, health−care personnel, volunteers and government agencies.
Source: http://www.herald−dispatch.com/apps/pbcs.dll/article?AID=/20060404/NEWS01/604040308/1001/NEWS

[Return to top]

Information Technology and Telecommunications Sector

40. *April 05, Computer World* — **Apple unveils software that lets Macs run Windows.** Apple Computer Inc. Wednesday, April 5, unveiled a public beta of "Boot Camp," a software that allows its latest Intel−based Macintosh desktop and laptop machines to run Windows XP

natively. The software creates a hard−drive partition for Windows XP and lets users choose between the two operating systems at start−up time. It's available now as a free trial beta that works only for a limited time, and it will be included in the next major version of Mac OS X Version 10.5, or "Leopard," which is due out late this year. The software, which Apple released Wednesday with little fanfare, is available for free download immediately. Some Mac features won't work because of hardware incompatibilities, Apple said, including its remote control, wireless keyboard and mouse and the USB modem.
Source: http://www.computerworld.com/softwaretopics/os/macos/story/0,10801,110220,00.html

41. *April 05, Newsfactor Magazine* — **Microsoft offers free virtual server.** Virtualization is widely recognized as a way companies can slash IT infrastructure costs. By using the technology, IT administrators can replace larger, mostly unused servers with smaller, efficient machines that run multiple operating systems. In offering Virtual Server 2005 R2 as a no−charge download, Microsoft hopes to remove the barriers to adoption for customers who want to realize the benefits of these systems. Analysts have said it is only a matter of time before virtualization capabilities are commoditized, as chipmakers like Intel and AMD provide additional support for the technology at the motherboard level. This trend could mean that the battle for the virtualization market could shift entirely to software tools that help manage virtual environments and organize the systems to use the hardware more efficiently.
Source: http://www.newsfactor.com/story.xhtml?story_id=01100000A1LL&_page=1

42. *April 05, Security Focus* — **Sendmail asynchronous signal handling remote code execution vulnerability.** Sendmail is prone to a remote code execution vulnerability. Analysis: Compromise of networks and machines using affected versions of Sendmail may lead to exposure of confidential information, loss of productivity, and further network compromising. An attacker does not need to entice any kind of user interaction to trigger this vulnerability. Successful exploitation would grant an attacker the privileges that the Sendmail server daemon is running with. For a complete list of vulnerable products:
http://www.securityfocus.com/bid/17192/info
Solution: The vendor has released version 8.13.6 to address this issue.
For further solution details: http://www.securityfocus.com/bid/17192/solution
Source: http://www.securityfocus.com/bid/17192/references

43. *April 05, Government Accountability Office* — **GAO−06−425: Telecommunications: Weaknesses in Procedures and Performance Management Hinder Junk Fax Enforcement (Report).** The Telephone Consumer Protection Act of 1991 prohibited invasive telemarketing practices, including the faxing of unsolicited advertisements, known as “junk faxes,” to individual consumers and businesses. Junk faxes create costs for consumers (paper and toner) and disrupt their fax operations. The Junk Fax Prevention Act of 2005 clarified an established business relationship exemption, specified opt−out procedures for consumers, and requires the Federal Communications Commission (FCC) −− the federal agency responsible for junk fax enforcement −− to report annually to Congress on junk fax complaints and enforcement. The law also required the Government Accountability Office (GAO) to report to Congress on FCC’s enforcement of the junk fax laws. This report addresses (1) FCC’s junk fax procedures and outcomes, (2) the strengths and weaknesses of FCC’s procedures, and (3) FCC’s junk fax management challenges. GAO recommends that FCC revise its junk fax guidance for

consumers, develop data management strategies, and implement recognized performance management practices in carrying out its junk fax responsibilities. FCC officials said they generally concur with the recommendations. FCC also provided technical comments that were incorporated throughout this report as appropriate.
Highlights: http://www.gao.gov/highlights/d06425high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−425

44. *April 04, Federal Computer Week* — **Nevada unveils info−sharing system.** Several state and local governments and agencies in Nevada are participating in a new project that would allow them to share backup and systems recovery technology. Governor Kenny Guinn unveiled on Monday, April 3, the Nevada Shared Information Technologies Services project, which is being touted as a first−of−its−kind model to allow agencies to participate in shared−use facilities. State officials said this could be replicated nationwide to boost computer security.
Source: http://www.fcw.com/article92829−04−04−06−Web

45. *April 04, Security Focus* — **Linux kernel IP ID information disclosure weakness.** The Linux kernel is susceptible to a remote information disclosure weakness. This issue is due to an implementation flaw of a zero 'ip_id' information disclosure countermeasure. This issue allows remote attackers to use affected computers in stealth network port and trust scans. The replies to TCP SYN packets contain a correct IP ID value of zero, but replies to TCP SYNACK packets have an incremental IP ID field instead. This means a remote attacker can abuse this behavior for malicious purposes to perform an idle scan with nmap.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/17109/info
Solution: Various Linux kernel versions, such as some in the 2.4 series, are not affected by this issue. The vendor has released version 2.6.16.1 of the Linux kernel to address this issue. For further solution details: http://www.securityfocus.com/bid/17109/solution
Source: http://www.securityfocus.com/bid/17109/references

46. *April 04, Security Focus* — **McAfee WebShield SMTP remote format string vulnerability.** McAfee WebShield SMTP 4.5 MR1a is susceptible to a remote format string vulnerability. There exists a format string vulnerability within the McAfee WebShield SMTP server which allows an attacker to execute arbitrary code on the host computer via an unauthenticated connection. With successful exploitation, an unauthenticated attacker is able to obtain SYSTEM access.
Solution: The vendor has released a patch (P0803), along with version 4.5 MR2 to address this issue. Users of affected packages should contact the vendor for further information on obtaining fixes.
Source: http://www.securityfocus.com/bid/16742/references

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may either allow an attacker to obtain sensitive data from stored cookies or redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur. For more information about the reported vulnerability can be found in the following:

CA−2000−02 CERT Advisory: Malicious HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA−2000−02.html

VU#808921 US−CERT Vulnerability Note: eBay contains a cross site scripting vulnerability http://www.kb.cert.org/vuls/id/808921

US−CERT recommends the following:

Disable Scripting as specified in the Securing Your Web Browser document at URL: http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

The Malicious Web Scripts FAQ information at URL:http://www.cert.org/tech_tips/malicious_code_FAQ.html#st eps

Validate web site addresses as described in the eBay Spoof Email Tutorial information at URL: http://www.microsoft.com/technet/security/advisory/917077.mspx

ST04−014 US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST04−014.html

ST05−010 Validate web site certificates as described in US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST05−010.html

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target	27754 (−−−), 1026 (win−rpc), 6881 (bittorrent), 3800 (−−−), 25 (smtp), 445 (microsoft−ds), 41170 (−−−), 32768 (HackersParadise), 32459

Ports	(−−−), 6348 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

47. *April 05, Associated Press* — **California levees break, flooding trailer park.** Two levees broke Tuesday, April 4, in California's chief agricultural region, flooding a trailer park, threatening other homes in Merced and inundating farmland near Sacramento. There were no immediate reports of any injuries across the Central Valley. The breaks occurred as rain continued to fall across Northern California, with some residents evacuating their homes near San Francisco because of the threat of landslides and forecasters predicting continued wet weather for two more weeks. Water breached a 30−foot section of levee along a creek in Merced, sending up to 18 inches of water pouring through a mobile home park, said Michael Miller, a spokesperson for the Department of Water Resources. Three trailer parks were evacuated, a total of 200 people, said Elaine Post, spokesperson for the Merced County Office of Emergency Services.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=48196

48. *April 05, Associated Press* — **Smart cameras and armed guards to protect WTC site.** At the new and rebuilt World Trade Center (WTC) site visitors might submit to an iris scan or an analysis of their thumb print to get into buildings, while smart cameras try to match their faces to a photo database of known terrorists. Well−paid, armed guards would be on patrol while sensors test the air for lethal gases. Preliminary details of a plan to make the redeveloped 16−acre site as terrorism−proof as possible were provided by former FBI agent James Kallstrom, Governor George Pataki's senior counterterrorism adviser. Kallstrom and New York city and federal officials are aiming for a standard of security that doesn't yet exist in public spaces around the nation. "This'll be reflective of the times we live in," said Kallstrom. "The consequences of attacking here could have more significance to the terrorists. It has a lot of symbolism. It's going to be extremely well protected." The plan is taking shape while construction begins this spring on a memorial to the 2001 terrorist attacks and the Freedom Tower, a 1,776−foot skyscraper that some say is having trouble attracting tenants because of security concerns. A transit hub, performing arts center and more office towers are also planned.
Source: http://www.chiefengineer.org/content/content_display.cfm/seqnumber_content/2437.htm

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer